Audit Report

OFFICE OF THE INSPECTOR GENERAL

CONTROLS OVER APPLICATION SOFTWARE
SUPPORTING THE NAVY'S INVENTORIES
HELD FOR SALE (NET)

Report No. 95-066   December 30, 1994

20000301 022

Department of Defense

AQI00-06-1386

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

> Inspector General, Department of Defense
> OAIG-AUD (ATTN: APTS Audit Suggestions)
> 400 Army Navy Drive (Room 801)
> Arlington, Virginia 22202-2884

DoD Hotline

To report fraud, waste, or abuse, call the DoD Hotline at (800) 424-9098 (DSN 664-8567) or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

Acronyms

DBOF	Defense Business Operations Fund
DISA	Defense Information Systems Agency
DISA-WESTHEM	Defense Information Systems Agency-Western Hemisphere
DISO	Defense Information Services Organization
DMC	Defense Megacenter
FMSO	Fleet Material Support Office
IBM	International Business Machines Corporation
ID	Identification
IG	Inspector General
CA-IDMS	Computer Associates, Inc., Integrated Data Management System
SPCC	Ships Parts Control Center

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

December 30, 1994

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT)
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Controls Over Application Software Supporting the
Navy's Inventories Held for Sale (Net) (Report No. 95-066)

This audit was made in support of the audit of the FY 1994 consolidated
financial statements for the Navy's Defense Business Operations Fund. We are
providing this final report for your review and comments. In preparing the final
report, we considered comments made by the Assistant Secretary of the Navy
(Research, Development and Acquisition) for the Department of the Navy, and from
the Defense Information Systems Agency's Inspector General on behalf of the Defense
Megacenter-Mechanicsburg.

DoD Directive 7650.3 requires that all recommendations be promptly resolved.
Therefore, we request that the Navy and the Defense Information Systems Agency
provide comments on the final report by February 28, 1995. See the "Response
Requirements for Recommendations" chart at the end of Finding B for the unresolved
recommendations and the specific requirements for your comments.

The courtesies extended to our audit staff are appreciated. If you have any
questions about this audit, please contact Mr. David C. Funk, Audit Program Director,
at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager,
at (303) 676-7393 (DSN 926-7393). Appendix D lists the distribution of this report.
The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Audit Report No. 95-066   December 30, 1994
(Project No. 3FD-2025)

CONTROLS OVER APPLICATION
SOFTWARE SUPPORTING THE NAVY'S
INVENTORIES HELD FOR SALE (NET)

EXECUTIVE SUMMARY

Introduction. This audit was made in support of the audit of the FY 1994 consolidated financial statements for the Navy's Defense Business Operations Fund (the Fund). The audit focused on the Navy's PX06 Inventory Accounting and Billing application, including its interface with the PX02 Allotment and Accrual Accounting application. The Navy's two inventory control points use those applications to process financial data for wholesale and retail inventories. Wholesale inventories of $18.2 billion, classified as Inventories Held for Sale (Net), were reported on the Navy's consolidated financial statements for the Fund as of September 30, 1993. The following organizations in Mechanicsburg, Pennsylvania, were audited: the Navy Ships Parts Control Center (SPCC); the Navy Fleet Material Support Office (FMSO); and the Defense Information Systems Agency-Western Hemisphere[1] (DISA-WESTHEM), Defense Megacenter-Mechanicsburg (DMC-Mechanicsburg).

Objectives. Our objective was to determine the effectiveness of application controls and selected general controls over the Navy's PX06 application, and its interface with the PX02 application, in processing financial data reported as wholesale inventories on the Navy's consolidated FY 1994 financial statements for the Fund. The audit also evaluated the effectiveness of applicable internal controls and each organization's implementation of the DoD Internal Management Control Program as it pertained to our audit objectives.

Audit Results. Adequate application controls existed over the PX06 application and its interface with the PX02 application. The FMSO and the SPCC properly controlled changes to the PX06 application programs. The DMC-Mechanicsburg also followed adequate contingency planning practices by periodically backing up the operating system and PX06 application libraries. Although reliable application controls existed over the PX06 application, the application's integrity was compromised by a material weakness in the operating system. During our audit, the Defense Information Systems Agency created a task force to improve information systems security at the DMC-Mechanicsburg and other organizations of DISA-WESTHEM. See Part II, Prior Audits and Other Reviews, for a discussion of the task force's work. Because of their sensitive nature, the deficiencies summarized below and detailed in Part II of the report are discussed in general terms only. Details of our findings were separately provided to management.

     o The PX06 application was well-documented, operated as designed, and met the Navy's control objectives. After the DMC-Mechanicsburg corrects the material

---

[1]In October 1994, the Defense Information Services Organization was reorganized as the Defense Information Systems Agency-Western Hemisphere.

\

weakness discussed below, the PX06 application can be relied on to effectively process financial data reported as wholesale inventories on the Navy's FY 1994 financial statements for the Fund (Finding A).[2]

     o The general controls environment was inadequate. Weaknesses existed in general controls over the test and production systems supporting the PX06 application at the SPCC and the DMC-Mechanicsburg. As a result, the PX06 application programs and inventory accounting data could be improperly accessed, modified, or destroyed by knowledgeable users without risk of detection, thus jeopardizing the integrity of the system that processes the Navy's wholesale inventory (Finding B).

Internal Controls. A material internal control weakness existed in the general controls over sensitive operating system features. Inadequate controls over the operating system made it possible for knowledgeable users to improperly access, modify, or destroy sensitive computer data and programs without risk of detection. The DoD Internal Management Control Program was effectively implemented at the SPCC and the FMSO, but not at the DMC-Mechanicsburg. Additional details are provided in Part I (Internal Controls) and Part II (Finding B) of this report.

Compliance With Laws and Regulations. The requirements of the DoD Internal Management Control Program were met at both Navy organizations but not at the DMC-Mechanicsburg. The DMC-Mechanicsburg and the SPCC did not fully comply with other laws and regulations. Additional details are provided in Part I (Compliance With Laws and Regulations) and Part II (Finding B) of this report.

Potential Benefits of Audit. Opportunities for improving internal controls over computer operations existed at two organizations, but the related monetary benefits could not be quantified. Five recommendations will help to improve the general controls designed to limit user access to sensitive software. See Appendix B for a summary of the benefits resulting from this audit.

Summary of Recommendations, Management Comments, and Audit Response. We recommended that general controls be strengthened over the security software, the operating system, and the Computer Associates, Incorporated, Integrated Data Management System database for the test and production systems supporting the PX06 application at the SPCC and DMC-Mechanicsburg. The Navy concurred with the findings and recommendations, except for stating that one recommendation should have been directed to DISA. We disagree, and provided further explanation for consideration by the Navy. The Defense Information Systems Agency concurred with all findings and recommendations, including the material internal control weakness identified by the audit. We request that the Navy and DISA provide comments on this final report by February 28, 1995. See Part II for our response to management's comments, and Part IV for the complete text of the comments.

---

[2]Our audit was conducted in a test environment and did not include an evaluation of data inputs by the wholesale stock points. Therefore, additional audit tests are required before an opinion can be expressed on the wholesale inventory amounts reported on the Navy's FY 1994 financial statements for the Fund.

Table of Contents

Part I - Introduction

Background

This audit was made in support of the Naval Audit Service's audit of the FY 1994 consolidated financial statements of the Navy's Defense Business Operations Fund (DBOF). Supply management is one of the primary business areas that make up the Navy's portion of the DBOF. The Navy's DBOF Statement of Financial Position as of September 30, 1993, reported $19.1 billion in inventory; of that amount, $18.2 billion consisted of wholesale inventories, reported as Inventories Held for Sale (Net). Such inventories are stored and maintained worldwide at wholesale stock points.

Supply Management. The Naval Supply Systems Command has overall responsibility for the Navy's supply management area, which is managed by two inventory control points: the Navy Ships Parts Control Center (SPCC) at Mechanicsburg, Pennsylvania, and the Navy Aviation Supply Office at Philadelphia, Pennsylvania. The Defense Information Systems Agency-Western Hemisphere[1] (DISA-WESTHEM), Defense Megacenter in Mechanicsburg, Pennsylvania (DMC-Mechanicsburg), provides automated data processing support to the SPCC and the Navy Fleet Material Support Office (FMSO) in Mechanicsburg, Pennsylvania. By FY 1995, the DMC-Mechanicsburg will also provide automated data processing support for the Aviation Supply Office.

Inventory Application. The audit concentrated on the Navy's PX06 application, including its interface with the PX02 Allotment and Accrual Accounting application. The two Navy inventory control points use this application to process financial data on wholesale and retail inventories. The PX06 application replaced the financial control modules of the Uniform Automated Data Processing System at the SPCC. The SPCC began using the PX06 application in April 1993, followed by the Aviation Supply Office in December 1993. The PX06 application interfaces with several other applications, including the Uniform Automated Data Processing System and the PX02 Allotment and Accrual Accounting application. The FMSO is the central design activity for both the PX06 and PX02 applications.

To ensure the integrity of financial information derived from the PX06 application, adequate management controls must exist over the operating system and security software, as well as software that runs the database management system.

Operating System. The SPCC PX06 Production-Only System (the Production System) and the Development and Test Guest System (the Test System) are supported by two MADAM 5995 mainframe computers operated by personnel at the DMC-Mechanicsburg. The Multiple Virtual Storage/Extended Architecture operating system (the Operating System) was installed on the Test and Production Systems to control the execution of computer programs.

---

[1]In October 1994, the Defense Information Services Organization was reorganized as the Defense Information Systems Agency-Western Hemisphere.

An operating system is a major component of any computer system. It is an integrated collection of computer programs, service routines, and supervisory procedures that direct the sequence and processing of computer applications (that is, scheduling jobs, loading programs, allocating computer memory, managing libraries, and controlling input and output operations). An operating system also separates and protects individual user programs.

When the various features in an operating system are properly administered and controlled, only authorized programs can modify the processing of other programs. However, an operating system is not intended to ensure that only authorized users can execute authorized programs. Access control is achieved by using commercial security software to control authorized users. The security software is optional, but is needed to help preserve a system's integrity.

Security Software. Under license from the International Business Machines Corporation (IBM), the DMC-Mechanicsburg uses Resource Access Control Facility security software (the Security Software) to limit user access to computer processing capabilities, programs, data, and other computer resources. When properly installed and administered, the Security Software will protect a variety of computer resources and subsystems of the Operating System.

Database Management System. Computer Associates, Inc., Integrated Data Management System (CA-IDMS) is the database management system used to support the SPCC applications. CA-IDMS controls and organizes all data used and allows the data to be rearranged to suit different applications. CA-IDMS software must be properly installed to limit user access to the PX06 application and database.

Technical Terms. Other technical terms used in this report are defined in the Glossary (Appendix A).

Objectives

Overall and Specific Objectives. The overall objective of our audit was to determine the effectiveness of the application controls over the Navy's PX06 application (and its interface with the PX02 application) in processing financial data reported as Inventories Held for Sale (Net) on the FY 1994 consolidated financial statements for the Navy's DBOF. Specifically, for selected high-risk programs, the audit determined the effectiveness of the application controls intended to verify that original data input into the PX06 application were accurately entered and correctly processed, and that the application's outputs were adequately checked. The audit also evaluated the effectiveness of selected general controls affecting the integrity of the application. In addition, the audit evaluated the effectiveness of applicable internal controls and of each organization's implementation of the Internal Management Control Program as it pertained to our audit objectives.

Revision of Audit Objectives. During the audit, our original objectives were revised to reflect adjustments to the audit scope and the realignment of automated data processing support at the Naval Supply Systems Command. To better focus our audit resources, we limited the scope of our audit to the PX06 application (and its PX02 interface) used by the SPCC. Because we did not audit the Uniform Automated Data Processing System application used by the wholesale stock points, we could not determine whether data inputs by the wholesale stock points were properly authorized. So that the audit could concentrate on higher-risk areas, we also did not verify whether computer outputs from the PX06 and PX02 applications were properly distributed.

The Aviation Supply Office was excluded from our audit scope for two reasons. First, the PX06 application that the FMSO provides to the Aviation Supply Office is the same as that provided to the SPCC. Subject to verifying that the same software versions were in use at both locations, the audit determination made on the PX06 application used by the SPCC would also apply to the Aviation Supply Office. Second, the audit excluded the Aviation Supply Office to minimize additional disruptions to its operations. Disruptions were anticipated because of the transition to the PX06 application in December 1993 and the transfer of the Aviation Supply Office's automated data processing support to the DMC-Mechanicsburg, which was expected in November 1994.

Scope and Methodology

We performed audit work at the SPCC, the FMSO, and the DMC-Mechanicsburg. We examined the input, processing, and output controls over the PX06 application used by the SPCC, including its interface with the PX02 application, by using a test environment to duplicate the operating conditions of the SPCC Production System. We also evaluated general controls that could affect the integrity of the PX06 application. The general controls were controls over library access, supervisor calls, and sensitive utilities; and implementation of the Security Software features such as attributes and access protection. Application change controls and contingency (backup) planning were evaluated. An evaluation was also made of CA-IDMS controls over integrated data dictionaries, access to the PX06 application, CA-IDMS libraries, and utility programs.

Computer-Processed Data Used. To achieve the audit objectives, the audit relied on computer-processed data in the Operating System libraries and in the Security Software that support the SPCC Production and Test Systems. The audit used Computer Associates, Incorporated, EXAMINE auditing software to extract data directly from computer memory and the operating system libraries. Computer Associates, Incorporated, EXAMINE is a software program that audits the Operating System. The audit also used the Computer Associates, Incorporated, CULPRIT report writer to extract data directly from the CA-IDMS test database and the integrated data dictionary. All system and application testing was done in controlled environments with management's approval. The audit used automated and manual techniques to analyze the

Operating System and data from test transactions. Based on those tests and assessments, the data were sufficiently reliable to meet the audit objectives.

Time Period, Locations, and Standards. This financial-related audit was performed from October 1993 through May 1994. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General (IG), DoD, and accordingly included such tests of internal controls as were considered necessary. During the audit, we visited or contacted the organizations shown in Appendix C.

Internal Controls

Adequacy of Internal Controls. The audit evaluated application controls over the PX06 application and its PX02 interface, and selected general controls over the Operating System, the Security Software, and the CA-IDMS. A material internal control weakness, as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, existed in the general controls over sensitive features of the Operating System. Inadequate controls over the Operating System made it possible for knowledgeable users to improperly access, modify, or destroy sensitive computer data and programs without detection. Implementing Recommendations B.3.a. and B.3.b. will correct the material weakness in controls over supervisor calls on the Operating System. Details are provided in Part II (Finding B) of this report. Strengthened internal controls and other nonmonetary benefits will be realized from implementing the recommendations, as shown in Appendix B.

Internal Control Programs. During FY 1993, the DoD Internal Management Control Program was effectively implemented at both Navy organizations, but was not implemented at the DMC-Mechanicsburg. None of the organizations' internal control programs identified or reviewed the Operating System, Security Software, and CA-IDMS features examined during the audit.

The DMC-Mechanicsburg periodically evaluated internal controls during FY 1993, and acted on the results of those evaluations. However, during FY 1993, the DMC-Mechanicsburg did not conduct the required risk assessments or provide an Annual Statement of Assurance to the Defense Information Services Organization (DISO) (now DISA-WESTHEM), its parent organization. The DMC-Mechanicsburg did not implement the internal control program because of confusion at DISO about its responsibilities for reporting on

the SPCC Data Processing Department (now the DMC-Mechanicsburg) when operational control was transferred to the Defense Information Technology Services Organization[2] in January 1993.

DISO officials believed that SPCC was responsible for reporting on the DMC-Mechanicsburg until the assets were capitalized. As a result, when the Defense Information Systems Agency (DISA) submitted its FY 1993 Annual Statement of Assurance to the Comptroller, Department of Defense (now the Under Secretary of Defense [Comptroller]), that statement did not include the DMC-Mechanicsburg. DISO officials stated that the DMC-Mechanicsburg was included in DISO's internal control program for FY 1994.

Compliance With Laws and Regulations

To obtain reasonable assurance that application controls and certain general controls effectively protected the integrity of inventory data in the PX06 application, the audit tested compliance with laws and regulations that may directly affect the account balance of Inventories Held for Sale (Net) as reported on the FY 1994 financial statements of the Navy's DBOF. The audit also tested other laws and regulations pertaining to database management system controls, application controls, general controls, and inventory accounting.

The audit reviewed management's process for evaluating and reporting on internal control and accounting systems, which is required by the DoD Internal Management Control Program. The audit also reviewed and tested policies, procedures, and systems for documenting and supporting financial data, access controls, and system security and integrity.

The results of our tests indicated that with respect to the items tested, the DMC-Mechanicsburg and the SPCC did not fully comply with Title 2, "General Accounting Office Policy and Procedures Manual for Guidance of Federal Agencies" and DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988. Title 2 and DoD Directive 5200.28 require accounting systems to include controls that ensure data integrity and protect software and data from unauthorized access, either deliberate or accidental. These Title 2 requirements are incorporated in DoD Manual 7220.9-M, the "DoD Accounting Manual," October 1983. Part II (Finding B) of this report gives additional details.

---

[2]In July 1993, the Defense Information Technology Services Organization was reorganized under DISO, which is now DISA-Western Hemisphere. Both organizations were elements of the Defense Information Systems Agency.

Prior Audits and Other Reviews

Audit Followup. On June 30, 1993, the Naval Audit Service issued Report No. 053-H-93, "Fiscal Year 1992 Consolidating Financial Statements of the Department of the Navy Defense Business Operations Fund." In Finding 7 of the report, Recommendation 19, the Naval Audit Service recommended that DBOF organizations establish inventories as an assessable unit under the Navy's management control program. We verified that the SPCC and the FMSO had complied with the Naval Audit Service's recommendation. No other follow-up action on prior audits was required.

Similar Conditions at Other Organizations. The IG, DoD, and the Air Force Audit Agency have reported general control weaknesses similar to those at the DMC-Mechanicsburg (discussed in Finding B) and at other DISA-WESTHEM organizations.

      IG, DoD, Reports. The IG, DoD, reported that supervisor calls, authorized program facility files, sensitive utility programs, and security software were inadequately controlled at five DISA-WESTHEM information processing centers in Columbus, Cleveland, and Dayton, Ohio; Indianapolis, Indiana; and Kansas City, Missouri. As in Recommendation B.1. in this report, the IG, DoD, recommended in prior audit reports that the DISA-WESTHEM develop the IBM-recommended installation integrity guidelines for data processing installations, and that the five DISA-WESTHEM installations comply with those guidelines. Additional details of those audit findings and recommendations are in the following IG, DoD, reports: Report No. 94-065, March 24, 1994; Report No. 93-133, June 30, 1993; and Report No. 93-002, October 2, 1992. All three reports are entitled "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service."

      Air Force Audit Agency Reports. The Air Force Audit Agency issued a report entitled "Data Processing Center (DPC) Operations and Security at the Air Force Accounting and Finance Center (AFAFC)," Project No. 00195410, on August 5, 1991. The report stated that at the Air Force Accounting and Finance Center (now DISA-WESTHEM DMC-Denver), the management of selected features of the operating system and security software was inadequate, and controls over data integrity and security needed improvement.

      Management's Corrective Actions. DISA-WESTHEM concurred with the IG, DoD, recommendations and began implementing them. In April 1994, DISA created a task force to improve information systems security at all Defense megacenters and other sites. By the end of FY 1995, DISA expects to complete corrective actions on the recommendations in the three IG, DoD, reports. The task force's plans did not specifically mention the Air Force Audit Agency report; however, DMC-Denver is included in the scope of the task force's work. The "MVS Security Technical Implementation Standards," issued by DISA on August 29, 1984 (as revised), also established the recommended installation integrity guidelines for data processing installations.

This page was left out of orignial document

8

Part II - Findings and Recommendations

Finding A.   Application Controls

The SPCC and the FMSO had adequate application controls over the PX06 Inventory Accounting and Billing application and its interface with the PX02 Allotment and Accrual Accounting application.   Program and system specifications for the PX06 application were well documented, and the application operated as designed and documented.   Audit tests of the input, processing, and output controls in 17 of the 209 PX06 application programs determined that computations, field checks, reasonableness tests, validity checking, and other control techniques supported the Navy's control objectives.   After the DMC-Mechanicsburg corrects the material weakness discussed in Finding B, the PX06 application can be relied on to effectively process data reported as Inventories Held for Sale (Net) on the FY 1994 consolidated financial statements for the Navy's DBOF.[3]

Background

Application Controls.   In batch and on-line computer operations, application controls are divided into three types: input, processing, and output controls. Input controls help to ensure the integrity of data during conversion into machine-readable format and entry into the application.   Processing controls help to verify the integrity of inputs processed by the computer to ensure that no data are added, lost, or altered during processing.   Data output controls help to safeguard the integrity of reports generated by the computer and ensure that such outputs are correctly distributed in a timely manner.   Outputs from the PX06 application include database records, changes and deletions, action items, general ledger postings, statistical and report data, and outgoing bills.

Test Environment.   The audit evaluated application controls over batch and on-line inventory transactions at the SPCC by using a test environment to duplicate the operating conditions of the SPCC Production System.   The PX06 test environment consisted of 10 percent of the historical production data.

PX06 Application.   In addition to other functions, the PX06 application processes all supply transactions that require posting to the general ledger or issuing a bill.   The application determines how each transaction will be posted to the general ledger and transmits the data to the PX02 Allotment Accrual and Accounting application for posting to the general ledgers for the DBOF or the Appropriation Purchase Account.

---

[3]Our audit was conducted in a test environment and did not include an evaluation of data inputs by the wholesale stock points.   Therefore, additional audit tests are required before an opinion can be expressed on the wholesale inventory amounts reported on the Navy's FY 1994 DBOF financial statements.

Transaction Testing

To determine whether input, processing, and output controls were adequate, inventory transactions were entered into the PX06 test environment and the outputs were then compared to expected results. The audit used program specifications as the criteria for identifying the control objectives and techniques established by management. Results of the audit tests are detailed below.

Input Controls. The audit introduced batch and on-line transactions to the PX06 test environment to test and evaluate the overall program logic of selected high-risk programs. For example, tests were made on batch transactions that consisted of material receipts, material receipts with turn-ins, and issue transaction items. On-line tests included validating data fields, entering and applying cash collections and adjustments, and creating general ledger transactions. Adjustments were made to certain batch and on-line transactions to verify that transactions were accurately sent to the appropriate subsystem for review and correction. In addition, the audit reviewed and evaluated all transactions to verify that only valid transactions were accepted for processing.

Processing Controls. The PX06 application accurately processed and posted test transactions to the proper general ledger accounts. The audit tested program logic to verify validation of issues, receipts, and calculated amounts; adequate review of data mismatches; consistent use of system table values; accuracy of reversing entries; appropriate tracking of adjustments; accurate creation of cash bills; and retrieval of general ledger balances.

Computer Associates, Incorporated, CULPRIT report writer was used to extract transaction data directly from the CA-IDMS database in the PX06 test environment.

Output Controls. The DBOF trial balance accounts affected by the test transactions were accurately produced for the accounting period tested, and reflected the expected differences on the month-end closing reports. The audit retrieved general ledger balances for each account and selectively reconciled financial records to supply and billing records. Reconciliation reports included reports by account number and accounting classification for inventories, unfilled customer orders, stock in-transit from customers, and accounts receivable.

Summary

Since application controls over the PX06 application were adequate, we are not making any recommendations.

Finding B.   General Controls

At the DMC-Mechanicsburg and SPCC, general control weaknesses in the Security Software, the Operating System, and the CA-IDMS database existed in the Test and Production Systems supporting the PX06 application.

The weaknesses in the Security Software and the Operating System occurred because managers at DMC-Mechanicsburg:

> o assigned a higher priority to other work requirements,

> o were unaware of the sensitivity of certain utility programs, and

> o had not implemented the IBM-recommended installation integrity guidelines for the Operating System.

The CA-IDMS control weaknesses were caused by:

> o inadequate oversight by the DMC-Mechanicsburg and the SPCC, and

> o excessive user access to CA-IDMS database functions.

As a result, knowledgeable users could improperly access, modify, or destroy the PX06 application programs and inventory accounting data, without risk of detection. Those access risks jeopardized the integrity of the system that processes the Navy's wholesale inventory, valued at $18.2 billion, on September 30, 1993. The inadequate controls over supervisor calls on the Operating System constitute a material internal control weakness.

Background

Security Software. Resource Access Control Facility security software is IBM software for access control security. To protect data, the Security Software identifies and verifies users entering the system; restricts access to protected resources; limits the capabilities of authorized users who have access to protected resources; and maintains logs and generates reports on security-related events.

Database Management System. The CA-IDMS uses an integrated data dictionary to maintain and control the database and other data resources. The integrated data dictionary must be monitored because it controls access to the PX06 application. In addition, batch controls, such as read access to CA-IDMS libraries, must be closely monitored to prevent batch users from having unauthorized access to update CA-IDMS data, programs, and utilities. To use

the CA-IDMS databases more effectively, the vendor has provided utilities for developing and maintaining database applications. Two examples of these utilities are the Applications Development System, which is used to create on-line application systems, and the Data Manipulation Language/On-Line, which is used to update data in the database and the integrated data dictionary. To help prevent unauthorized changes to programs and accounting data, CA-IDMS utilities need to be controlled.

Laws and Regulations. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, states that an automated information system must have a C2 security classification if the system processes sensitive unclassified information requiring controlled access protection. The security classification requirements are specified in DoD Standard 5200.28, "DoD Trusted Computer System Evaluation Criteria (C^3I)," December 26, 1985. Among other requirements, that Standard requires that all computer libraries be protected. Also, Title 2, "General Accounting Office Policy and Procedures Manual for Guidance of Federal Agencies" (Title 2), requires accounting systems to include controls that ensure the integrity of data; protect software and data from unauthorized access, either deliberate or inadvertent; and limit access to authorized individuals. These Title 2 requirements were incorporated into the "DoD Accounting Manual." As discussed below, the DMC-Mechanicsburg and the SPCC did not fully comply with the access control or other requirements of DoD Directive 5200.28 and Title 2.

Security Software Features

Library Access. The DMC-Mechanicsburg did not limit access to update CA-IDMS and authorized program facility libraries. For example, on the Production System, up to 131 user identifications (IDs) and 52 started procedures could update CA-IDMS system libraries. Started procedures are operating system jobs or application programs initiated from a computer operator's console. On the Test System, 110 user IDs and 71 started procedures could update CA-IDMS system libraries, while 100 user IDs on the Production and Test Systems had update access to an authorized program facility library. Further, separation of duties was compromised because as many as 11 FMSO personnel could update the CA-IDMS and authorized program facility libraries on the Production System. Security personnel were aware that library access was not properly limited. During our audit, the DMC-Mechanicsburg published but had not fully implemented local guidance on limiting access to authorized program facility libraries, and began limiting update access. However, the guidance did not discuss the need to control update access to CA-IDMS. Because of the problems with access control, authorized users could make unauthorized changes to CA-IDMS and authorized program facility libraries, and could modify or destroy PX06 application programs and inventory accounting records.

13

Operations Attribute. The DMC-Mechanicsburg did not limit the use of the operations attribute to the users who maintained system libraries.   The operations attribute was assigned to 84 user IDs on the Test System and 67 user IDs on the Production System.   Unrestricted use of the operations attribute could result in unauthorized changes to system libraries because this attribute allows users to copy or catalog a library, delete resources protected by the Security Software, or perform any other maintenance function with the Security Software.   Managers at the DMC-Mechanicsburg did not have adequate oversight of users whose security profiles included the operations attribute.   The DMC-Mechanicsburg agreed with our conclusion and took corrective action during the audit.

C2 Security Requirements. The Test and Production Systems did not meet the C2 security requirements in DoD Directive 5200.28 because the Security Software's protect-all option, which secures all libraries, was not activated. DoD Directive 5200.28 states that organizations can request waivers to the C2 security requirements to prevent adverse effects to operations; however, the DMC-Mechanicsburg had not requested waivers.   Waivers can be approved only if alternative safeguards achieve the required level of security.   Personnel at the DMC-Mechanicsburg were aware of the C2 security requirements, but stated that because of higher-priority requirements, they did not use the protect-all option.   Failure to activate this option increases the risk that sensitive libraries will be created without access protection.

Sensitive Utility Programs. At the DMC-Mechanicsburg, sensitive utility programs on the Test and Production Systems were not adequately controlled. Although the DMC-Mechanicsburg used the Security Software to limit access to selected utilities, access to four sensitive utilities on the Test and Production Systems was not limited.   Because sensitive utilities can be used to add, delete, or change production programs and accounting data, they must be adequately controlled.   When we showed officials at the DMC-Mechanicsburg how a simulated file could obtain sensitive capabilities, they used the security software to secure two utilities on the Production System and one utility on the Test System.   However, they did not secure the remaining sensitive utility on the Test System.

Operating System

Controls Over Supervisor Calls. A DoD contractor and system programmers at the DMC-Mechanicsburg had installed non-IBM supervisor calls that compromised the integrity of the Test and Production Systems.   Of the 22 supervisor calls reviewed, 9 supervisor calls on the Production System and 8 supervisor calls on the Test System presented significant exposure risks to system integrity, either because supervisor calls were not installed correctly or because local supervisor calls did not have adequate validity checks.   In addition, 2 of the 17 supervisor calls that presented exposure risks were obsolete.   Management agreed that the controls on the Operating System could be bypassed.   The DMC-Mechanicsburg was upgrading certain vendor-

added supervisor calls on the Test and Production Systems. If properly installed, the upgrades should correct the problems with nine supervisor calls.

Installation Integrity Guidelines for the Operating System. Installing the non-IBM supervisor calls on the Production and Test Systems compromised system integrity by exposing the two systems to greater risk of unauthorized access and the potential for circumventing security controls. Integrity was compromised because the DMC-Mechanicsburg had not implemented the IBM-recommended installation integrity guidelines for a Multiple Virtual Storage/Extended Architecture operating system on the Test and Production Systems. In response to recommendations made in prior IG, DoD, audit reports, the Defense Information Systems Agency issued these guidelines as the DISA-WESTHEM "MVS Security Technical Implementation Standards," on August 29, 1994 (as revised). See Part I, "Prior Audits and Other Reviews," for additional details. With the user- and vendor-added supervisor calls that had integrity exposures, knowledgeable users could bypass controls on the Operating System and Security Software and could add, modify, or delete data without detection. The inadequate controls over supervisor calls on the operating system constitute a material weakness as defined by DoD Directive 5010.38. These inadequate controls jeopardize the integrity of the PX06 application that processes the Navy's wholesale inventory, valued at $18.2 billion, on September 30, 1993.

Database Management System

Managers at the DMC-Mechanicsburg and the SPCC did not adequately control the integrated data dictionary; batch controls over access to CA-IDMS libraries; access to PX06 application functions; and CA-IDMS utilities.

The managers did not provide adequate oversight and improperly evaluated the potential risks. Consequently, knowledgeable users could improperly access, modify, or destroy application and accounting data files. These access problems jeopardized the integrity of the PX06 application that the inventory control points used to process the Navy's wholesale inventory.

Integrated Data Dictionary Controls. Systems programmers at the DMC-Mechanicsburg did not adequately maintain the integrated data dictionary for the Production System. Specifically, when securing the integrated data dictionaries on the Test and Production Systems, the programmers overlooked a secondary integrated data dictionary on the Production System. The DMC-Mechanicsburg secured seven other primary and secondary integrated data dictionaries on the Test and Production Systems. However, because one integrated data dictionary was not secured, application programs and data files were exposed to increased risk of unauthorized changes by knowledgeable users.

Batch Controls. Batch controls over access to CA-IDMS libraries did not prevent batch users from bypassing controls in the integrated data dictionary. Although the risk was low, 4,700 batch users in the Production System could

bypass integrated data dictionary controls when accessing the CA-IDMS database in the multiuser configuration, technically known as the Central Version mode. The Central Version mode is one of two modes in which batch jobs can access a CA-IDMS database. Because the DMC-Mechanicsburg gave all users read access to CA-IDMS libraries, batch users could update the database. Without strong batch controls, the risk increases that batch users may have unauthorized access to CA-IDMS data, programs, and utilities.

Application Access. The SPCC security personnel did not adequately limit access to the PX06 production application. Specifically, three development analysts and four database analysts had access to PX06 functions, such as "create" and "update", that should have been limited to application users. Nine users had duplicate user IDs. Seven of the nine users were former SPCC personnel who had user IDs for both the SPCC and the Defense Finance and Accounting Service. Two of the nine users were SPCC personnel who had access to the application under FMSO user IDs, which should have been removed at the end of their temporary assignments to the FMSO. In addition, four user IDs were assigned to personnel who no longer used the PX06 application. Numerous user IDs were assigned to individuals whose identities were unknown to security personnel. Finally, more than 70 user IDs had access to the PX06 function that allows on-line creation of a transaction. To meet the access control requirements of DoD Directive 5200.28 and DoD Manual 7220.9-M, the SPCC could have periodically reviewed the levels of access given to authorized users. Because the SPCC did not conduct such reviews, individuals were given inappropriate access to the PX06 production application, thus increasing the risk of unauthorized changes to data files in the PX06 application.

CA-IDMS Utility Controls. The SPCC database administrator did not adequately control two CA-IDMS utilities that could be used to modify database records or to make unauthorized changes to on-line applications. The two utilities were Data Manipulation Language/On-Line and the Application Development System. Although security classifications were assigned to tasks performed by Data Manipulation Language/On-Line and the Application Development System, access to the tasks was not limited to database administration personnel. Specifically, 9 of 18 personnel with access to Data Manipulation Language/On-Line, and 18 of 30 personnel with access to the Application Development System, were not database administration personnel. Inadequate oversight of those utilities increased the risk of unauthorized changes to programs and accounting data, including the PX06 application.

Summary

Because of the general control weaknesses discussed above, the PX06 application programs and inventory accounting data could be improperly accessed, modified, or destroyed by knowledgeable users without detection. The DMC-Mechanicsburg and the SPCC need to improve management

oversight, allow only authorized users to access the system, and make other operational changes to restore the integrity of the system that processes the Navy's wholesale inventory.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Megacenter-Mechanicsburg, fully implement the Defense Information Systems Agency-Western Hemisphere's "MVS Security Technical Implementation Standards," August 29, 1984 (as revised).

Management Comments: The DISA Inspector General concurred with the finding and recommendation and estimated that corrective actions would be completed by July 14, 1995. The recommendation was revised to cite the specific guidelines issued by DISA.

2. We recommend that the Information Systems Security Officer, Defense Megacenter-Mechanicsburg:

    a. Review and limit access to update the Computer Associates, Incorporated, Integrated Data Management System libraries and the authorized program facility libraries on the Test and Production Systems.

Management Comments: The DISA Inspector General concurred with the findings and recommendation and stated that corrective action was complete on March 31, 1994.

    b. Activate the protect-all option required for a C2 security rating on the Test and Production Systems, or obtain a waiver from the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) from the C2 security requirements established by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and estimated that corrective action would be completed by May 1, 1995.

    c. Review the use of all sensitive utilities and restrict their use with the Resource Access Control Facility.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and stated that corrective actions were complete on March 31, 1994.

3. We recommend that the Chiefs of the System Management Department and the Software Management Department, Defense Megacenter-Mechanicsburg:

    a. Develop adequate validity checking for locally-written supervisor calls to prevent unauthorized user operations and system requests that, if allowed, would compromise system security controls.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and estimated that corrective action would be completed by December 31, 1994.

    b. Remove obsolete supervisor calls and either correct improperly installed supervisor calls or replace the supervisor calls with planned upgrades.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and estimated that corrective action would be completed by December 31, 1994.

4. We recommend that the Chief, Software Management Department, Defense Megacenter-Mechanicsburg:

    a. Review the security measures for all primary and secondary integrated data dictionaries and make appropriate changes to verify that application programs and data are adequately protected.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and estimated that corrective actions would be completed by December 31, 1994.

    b. Allow only users with valid needs to have read access to certain Computer Associates, Incorporated, Integrated Data Management System libraries.

Management Comments: The DISA Inspector General concurred with the finding and recommendation and stated that corrective action will be taken.

Audit Response: The corrective actions proposed by DMC-Mechanicsburg are adequate. However, DMC-Mechanicsburg should provide completion dates for actions taken or planned. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

5. We recommend that the Commander, Naval Supply Systems Command, direct the Commanding Officer, Navy Ships Parts Control Center, to:

    a. Limit batch users with read access to certain Computer Associates, Incorporated, Integrated Data Management System libraries to those users having a valid need.

Management Comments: The Assistant Secretary of the Navy (Research, Development and Acquisition) (the Assistant Secretary) nonconcurred, stating that the recommendation should not have been addressed to the Navy. The Assistant Secretary stated that the DMC-Mechanicsburg was responsible for library control. She stated that limiting the number of batch users who have read access conflicts with the Navy's policy of increasing operational efficiency by providing as much CA-IDMS read capability as possible without corrupting the data. The Assistant Secretary also stated that the security features of the database management system adequately limited access to authorized users.

Audit Response: We do not agree that the SPCC has no responsibility for controlling batch users' access to the database management system. A collaborative role should exist between the SPCC and the DMC-Mechanicsburg in controlling the access of CA-IDMS batch users. As the user of the database management system, the SPCC is responsible for informing the DMC-Mechanicsburg of the batch users who should have access to the system and the extent of such access. The DMC-Mechanicsburg is responsible for making the necessary adjustments to the Security Software to limit batch users' access.

To increase operational efficiency, the Navy can grant read access to all CA-IDMS batch users. However, by doing so the Navy accepts the low but potentially costly risk that the database may be corrupted. We disagree with the Navy position to grant universal access to batch users. While we understand the Navy rationale for granting the access, the CA-IDMS Version 10.2 used by the DMC-Mechanicsburg was susceptible to deliberate corruption by batch users. That software version provided only limited means of controlling batch users' access. When the database management system is upgraded to CA-IDMS Version 12.0, the risk to database integrity could be significantly reduced, if access controls are fully implemented. When that upgrade is completed, however, the SPCC will still have greater responsibility for controlling the access of CA-IDMS batch users.

CA-IDMS Version 12.0 uses three methods to control batch users' access:

   o the Security Software,

   o the integrated data dictionary, and

   o new internal security-checking features.

With input from the SPCC, the DMC-Mechanicsburg is responsible for maintaining the Security Software. The SPCC will share responsibility with the DMC-Mechanicsburg for controlling and maintaining the integrated data dictionary. The SPCC will also have primary responsibility for managing the new internal security-checking features of CA-IDMS Version 12.0. Therefore, we request that the Navy reconsider its position concerning the SPCC responsibilities for controlling the access of CA-IDMS batch users, and provide comments by February 28, 1995. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

b. Limit the access of authorized users to the PX06 application's functions, and periodically review and validate access to the PX06 application.

Management Comments: The Assistant Secretary of the Navy (Research, Development and Acquisition) concurred with the finding and recommendation. On August 30, 1994, the SPCC and the DMC-Mechanicsburg completed a review of authorized users. Appropriate adjustments to the security system were being made, and procedures had been established to conduct semiannual reviews of user access.

c. Allow only database administration personnel to have access to the Application Development System and Data Manipulation Language/On-Line utilities.

Management Comments: The Assistant Secretary of the Navy (Research, Development and Acquisition) concurred with the finding and recommendation. Users have been denied access to the Application Development System utility. For the Data Manipulation Language/On-Line utility, appropriate changes to user access will be made by March 31, 1995.

<u>Response Requirements for Each Recommendation</u>

Responses to the final report are required from the addressees shown for the items indicated with "X" in the chart below.

		Response Should Cover:			
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues
4.b.	DISA[1]			X	NA
5.a.	Navy[2]	X	X	X	NA

[1]DISA = DISA-Western Hemisphere, DMC-Mechanicsburg.
[2]Navy = Naval Supply Systems Command.

Part III - Additional Information

Appendix A. Glossary

Access control is a general term used to describe a number of techniques that restrict users of a computer system from gaining access to the system or other users' data or from performing unauthorized actions. When applied to software, access control usually refers to a specialized software security package, such as Resource Access Control Facility.

Authorized program facility is an IBM mechanism for protecting the integrity and security of the Multiple Virtual Storage operating system. The authorized program facility provides for the orderly, controlled extension of the operating system by defining special program libraries that may contain programs authorized to execute in the computer's supervisor state, which allows the program to execute all machine instructions. Programs operating in the supervisor state have the potential to bypass all security controls.

Only properly authorized programs should be allowed to perform sensitive tasks, such as accessing or modifying another program's execution or data areas. When a program can perform sensitive functions outside established authorized program facility rules, the program can become part of the operating system and can then circumvent or disable all security mechanisms, alter audit trails, or modify computerized data, regardless of the presence of access control software.

According to the IBM Multiple Virtual Storage security manual, authorized program facility procedures should require system programmers to use security software to control the creation of and access to authorized program facility libraries and the creation of authorized program facility programs. All authorized program facility programs should have unique names to prevent mix-ups in processing, and the file containing the names of authorized program facility libraries and volume serial numbers (disk device numbers) should reflect only valid libraries and volume serial numbers. Failure to comply with the IBM guidelines can significantly compromise the integrity of the operating system and can lessen management's control over system software.

Application programs are programs that are intended to serve particular business or nonbusiness needs and have specific input, processing, and output activities. Accounts receivable, general ledger, payroll, and personnel programs are some types of application programs.

Batch processing is the execution of a program or set of programs on the basis of a single initiating action.

Computer Associates, Incorporated, CULPRIT is a report writer that can extract data directly from a CA-IDMS database and the integrated data dictionary.

Computer Associates, Incorporated, Integrated Data Management System (CA-IDMS) provides utilities to control and organize all data used, while allowing the data to be rearranged to suit different applications. All data

22

records are stored in a database, which is a central repository for each application. CA-IDMS, a dictionary-driven database management system, uses an active data dictionary that contains information used to control the execution of the database management's components.

Database is a collection of interrelated data that are stored together.

Database management system is a software system that facilitates the creation and maintenance of a database and the execution of computer programs using the database. Computer Associates, Incorporated, Integrated Data Management System is one of many types of database management systems available commercially.

Disk is a data storage device that allows data to be accessed randomly or sequentially without passing through unwanted data.

Field checks are edit checks in which the characters in a field are examined to make sure they are of the correct field type (such as numeric data in numeric fields).

File is a collection of related data records stored on an external storage medium, usually a disk or tape.

Integrated data dictionary controls and directs outputs and actively documents the source and use of all data; definitions need not be duplicated, and all database management system and data communication components can use integrated data dictionary definitions.

Job is a basic unit of work on an IBM computer. A job consists of one or more steps or program executions.

Library is a collection of related data files or programs.

Multiple Virtual Storage/Extended Architecture operating system is one of two major operating systems that run on large IBM mainframe computers. The other major IBM operating system is known as the Virtual Machine operating system.

On-line processing means that individual transactions are processed as they occur and from their point of origin, rather than accumulated and then processed in batches.

Operations attribute is one of several attributes in the Resource Access Control Facility (the Security Software) user profile that define certain capabilities or limitations of users. Unless specifically restricted, the operations attribute gives users access to resources that are protected by Security Software. Unrestricted use of that attribute could result in unauthorized changes to system libraries because the operations attribute allows users to copy or catalog a library, delete resources protected by the Security Software, or perform any other maintenance function with the Security Software.

Read access is a security feature that allows a user only to read, execute, or copy a file.

Reasonableness tests are edit checks of the logical correctness of relationships among the values of data items on an input record and the corresponding file record. For example, a journal entry that debits inventory and credits wages payable is not reasonable because such transactions do not occur.

Sensitive utilities are computer programs that provide general support for computerized processes (such as diagnostic programs or programs designed to create test data or copy data from one storage device to another). The utilities become sensitive when they can bypass the system's security software or internal controls and thereby destroy data if not used properly.

Software is a generic term used to define all programming on a computer system, whether supplied by vendors or developed by in-house programmers. System software includes the operating system and accompanying utility programs that enable users to control, configure, and maintain the computer system.

Started procedure is an operating system job or application program initiated from an operator console.

Supervisor call is an assembler language instruction that causes a hardware interruption when executed. The operating system then passes control to the supervisor call to inform the operating system of the service (open a file for read or write access, close a file, etc.) that is being requested.

Supervisor calls are divided into two categories. One category is available to all programs, while the second is restricted to those programs authorized by the authorized program facility. Validity checking is the control technique that limits the execution of sensitive, unrestricted supervisor calls. The first 200 supervisor calls are provided by IBM or other software vendors. The remaining 56 supervisor calls can be added by a computer center's in-house programmers to meet its unique requirements or a vendor's software requirements.

Update access is a security system feature that allows write access to a file.

User identification is a method by which users sign on to a computer system and are identified. An individual user could have more than one user ID. Access to a computer system should require the input of both a valid user ID and a password.

Utility programs are computer programs or routines that perform general data- and system-related functions (such as copying, sorting, and merging files) required by other application software, the operating system, or users.

Validity checking is an integrity control used in a Multiple Virtual Storage/Extended Architecture operating system environment. It detects and disallows invalid user operations and system requests that could compromise

security controls. In an application environment, validity checking refers to testing the validity of codes, such as account numbers, transaction numbers, or vendor numbers.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
B.1.	Internal controls. Implements IBM-recommended installation integrity guidelines to provide better control of system data.	Nonmonetary.
B.2.a. B.2.b. B.2.c.	Internal controls. Provides better control of system libraries, programs, and data by protecting system libraries, and by limiting update access to the database management system, authorized program facility libraries, and sensitive utilities.	Nonmonetary.
B.3.a. B.3.b.	Internal controls. Provides better control of system data by improving controls over sensitive supervisor calls.	Nonmonetary.
B.4.a. B.4.b.	Internal controls. Strengthens database controls over data dictionary; batch users; access to data, applications, and other software; and certain utilities.	Nonmonetary.
B.5.a. B.5.b. B.5.c.	Internal controls. Improves access controls over database security and users. Improves controls over sensitive database utilities. Reduces the risk of unauthorized access.	Nonmonetary.

Appendix C. Organizations Visited or Contacted

Department of the Navy

Naval Supply Systems Command, Arlington, VA
   Navy Fleet Material Support Office, Mechanicsburg, PA
   Navy Ships Parts Control Center, Mechanicsburg, PA
Naval Audit Service, Eastern Region, Cherry Hill, NJ

Defense Organizations

Defense Information Systems Agency, Arlington, VA
   Defense Information Services Organization,[1] Denver, CO
     Defense Megacenter,[2] Mechanicsburg, PA

Non-Defense Federal Organization

General Accounting Office, Washington, DC

---

[1]Now the Defense Information Systems Agency-Western Hemisphere.
[2]Now the DMC-Mechanicsburg, Defense Information Systems Agency-Western Hemisphere.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Deputy Under Secretary of Defense (Comptroller/Management Systems)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
   Deputy Assistant to the Secretary of Defense (Information Management)
Assistant to the Secretary of Defense (Public Affairs)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Secretary of the Navy
Assistant Secretary of the Navy (Research, Development and Acquisition)
Assistant Secretary of the Navy (Financial Management)
Comptroller of the Navy
Auditor General, Department of the Navy
   Director, Naval Audit Service, Eastern Region
Commander, Naval Supply Systems Command
   Commanding Officer, Navy Fleet Material Support Office
   Commanding Officer, Navy Ships Parts Control Center
      Command Evaluation Office, Navy Ships Parts Control Center

Department of the Air Force

Auditor General, Department of the Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
   Director, Defense Finance and Accounting Service Cleveland Center
Director, Defense Information Systems Agency
   Director, Defense Information Systems Agency-Western Hemisphere
      Director, Defense Megacenter-Mechanicsburg
Director, Defense Logistics Agency
Director, National Security Agency

Inspector General, Central Imagery Office
Inspector General, Defense Intelligence Agency
Inspector General, National Security Agency
Director, Defense Logistics Studies Information Exchange

Non-Defense Federal Organizations

Office of Management and Budget
Technical Information Center, National Security and International Affairs Division,
 General Accounting Office

Chairman and Ranking Minority Member of Each of the Following Congressional
 Committees and Subcommittees:

    Senate Committee on Appropriations
    Senate Subcommittee on Defense, Committee on Appropriations
    Senate Committee on Armed Services
    Senate Committee on Governmental Affairs
    House Committee on Appropriations
    House Subcommittee on Defense, Committee on Appropriations
    House Committee on Armed Services
    House Committee on Government Operations
    House Subcommittee on Legislation and National Security,
        Committee on Government Operations

This page was left out of orignial document

3D

Part IV - Management Comments

Department of the Navy Comments

THE ASSISTANT SECRETARY OF THE NAVY
(Research, Development and Acquisition)
WASHINGTON, D.C. 20350-1000

8 NOV 1994

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT INSPECTOR
GENERAL FOR AUDITING

Subj: DODIG DRAFT AUDIT REPORT ON CONTROLS OVER APPLICATION
SOFTWARE SUPPORTING THE NAVY'S INVENTORIES HELD FOR SALE
(NET) (PROJECT NO. 3FD-2025) - ACTION MEMORANDUM

Ref: (a) DODIG memo of 12 Aug 94

Encl: (1) Department of the Navy Response

I am responding to the draft audit report forwarded by
reference (a) concerning controls over application software
supporting the Navy's inventories held for sale (net).

The Department of the Navy response is provided at enclosure
(1). With one exception, as noted, we concur in the findings and
recommendations. Action has been or is being taken to correct
the weaknesses identified in the audit.

We do not, however, concur with recommendation 5a, for the
reasons stated in the enclosure. In any event, that
recommendation is properly within the cognizance of the Defense
Megacenter-Mechanicsburg. By copy of this memorandum, I request
that the Director, Defense Information Systems Agency take
recommendation 5a for action.

Nora Slatkin

Copy to:
DIRDISA
NAVINSGEN
NAVCOMPT(NCB-53)

32

DEPARTMENT OF THE NAVY RESPONSE
TO
DODIG DRAFT AUDIT REPORT
ON
CONTROLS OVER APPLICATION SOFTWARE SUPPORTING THE NAVY'S
INVENTORIES HELD FOR SALE (NET)
(PROJECT NO. 3FD-2025)

Finding A. Application Controls

The SPCC and the FMSO had adequate application controls over the PX06 Inventory and Accounting and Billing application (and its interface with the PX02 Allotment and Accrual Accounting application). Program and system specifications for the PX06 application were well documented, and the application operated as designed and documented. Audit tests of the input, processing and output controls in 17 of the 209 PX06 application programs determined that computations, field checks, reasonableness tests, validity checking, and other control techniques supported the Navy's program control objectives. After the DMC-Mechanicsburg corrects the material weakness discussed in Finding B, the PX06 application can be relied on to effectively process data reported as Inventories Held for Sale (Net) on the fiscal year 1994 consolidated financial statements for the Navy's Defense Business Operations Fund.

DON Comment

Concur.

Finding B. General Controls

General Control weaknesses in the Security Software, Operating Systems, and CA-IDMS data base existed in the Test and Production Systems supporting the PX06 application at the DMC-Mechanicsburg and the SPCC. The weaknesses in the Security Software and the Operating Systems occurred because DMC-Mechanicsburg managers assigned a higher priority to other work requirements, were unaware of the sensitivity of certain utility programs, and had not implemented the IBM-recommended installation integrity guidelines for the Operating Systems. The CA-IDMS control weaknesses were caused by inadequate oversight by the DMC-Mechanicsburg and the SPCC and by excessive user access to CA-IDMS database functions. As a result, the PX06 application programs and inventory accounting data could be improperly accessed, modified, or destroyed by knowledgeable users without risk of detection. Those access risks jeopardized the integrity of the system that processes the Navy's wholesale inventory, valued at $18.2 billion on September 30, 1993. The inadequate controls over supervisor calls on the Operating Systems constitute a material internal control weakness.

DON Comment

Concur.

Recommendations

5. We recommend that the Commander, Naval Supply Systems Command, direct the Commanding Officer, Navy Ships Parts Control Center, to:

    a. Limit batch users with read access to Computer Associates, Inc., Integrated Data Management System libraries to those users having a valid need.

DON Comment

Do not concur. Control of libraries is the responsibility of DMC-Mechanicsburg; therefore, the recommendation should be addressed to DISA. It is the Navy's policy to provide as much read capability as possible without corrupting the data. This reduces the labor required to address customer inquiries. Limiting batch users with read access conflicts with our policy. The system has adequate security to restrict users to what has been authorized, that is, read only capability.

    b. Limit the access of authorized users to the PX06 application functions, and periodically review and validate access to the PX06 application.

DON Comment

Concur. SPCC determines and assigns authorized users since the ownership of the data within the data bases resides with SPCC and DFAS, Cleveland Center. To satisfy this recommendation, DMC-Mechanicsburg and SPCC completed a review of authorized users on 30 August 1994. The appropriate adjustments to the security system are in process, and procedures are now in place to review the access of authorized users semiannually.

    c. Limit the users with access to the Application Development System and Data Manipulation Language/On-Line utilities to database administration personnel. /

DON Comment

Concur. While access to the Application Development System utility is not security-controlled (security profile allows user access), the task code has been disabled which denies the user access. While this may not be the ideal approach to secure ADS from the user, Naval Supply Systems Command supports the recommendation for limiting access to ADS. DMC-Mechanicsburg and SPCC are in the process of reviewing access to the Data Manipulation Language/On-Line utilities. Based on the review,

changes will be made to the users security profile.   Estimated
completion date of the review is 31 March 1995.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURT HOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO: Inspector General (DO2)   13 October 1994

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Financial Management Directorate

SUBJECT: Draft Audit Report on Controls Over Application Software
                Supporting the Navy's Inventories Held for Sale (Net)
                (Project No. 3FD-2025)

Reference: DoDIG Audit Report, subject as above, 12 Aug 94

1. The referenced report requests we provide comments on deficiencies in general controls over test and production systems supporting the inventory application at the Defense Megacenter (DMC) Mechanicsburg. We reviewed the report and concur with the finding and its recommendations for DMC Mechanicsburg. Management comments and a description of corrective actions underway at the DMC are enclosed.

2. The point of contact for this action is Ms. Sandra Leicht, Audit Liaison. If you have questions on our response, Ms. Leicht can be reached at commercial (703) 692-5326 or DSN 222-5326.

FOR THE DIRECTOR:

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

**MANAGEMENT COMMENTS ON CONTROLS OVER APPLICATION
SOFTWARE SUPPORTING THE NAVY'S INVENTORIES
HELD FOR SALE (NET) (PROJECT NO. 3FD-2025)
COMMENTS TO FINDING B**

1. Recommendation 1 - Concur. The Director, DMC Mechanicsburg will fully implement the installation integrity guidelines as recommended by IBM. The following general plan is provided to implement the recommendation:

    a. Develop Director's policy letter on implementing installation integrity guidelines. Estimated completion date is 1 November 1994.

    b. Develop specific requirement profile from IBM recommendations and DISA policy and guidelines. Estimated completion date is 1 November 1994.

    c. Match current facility, practices and capabilities to the developed profile. Identify the requirements where there is full compliance, partial compliance, and lack of compliance and document results. Estimated completion date is 20 January 1995.

    d. Develop the plan to bring into full compliance those instances where there is either partial or no compliance. Include any investment costs associated with coming to compliance. Estimated completion date is 17 February 1995.

    e. Submit investment requirements, if any, to DISA WESTHEM. Estimated completion date is 24 February 1995.

    f. Bring "partial compliance" items to full compliance. Estimated completion date is 5 May 1995.

    g. Bring "no compliance" items to full compliance. Estimated completion date is 14 July 1995.

Estimated completion dates are subject to fluctuation depending the outcome of the compliance analysis and the costs and complexity of actions leading to compliance.

2. Recommendation 2 - Concur

    Recommendation 2.a.: Concur. We reviewed and limited access to the Integrated Data Management System (IDMS) and authorized program facility (APF) libraries on the Test and Production Systems. Access is now restricted to these libraries. This action was completed by 31 March 1994.

    Recommendation 2.b.: Concur. We will activate the "protect all" option required for a C2 security rating on the Test and Production Systems. There are over 4,000 data sets to be reviewed and access lists/protection to be added before "protect all" options can be turned on. This process should be completed 1 May 1995.

Recommendation 2.c: Concur. We reviewed the use of all sensitive utilities and restricted their use with the Resources Access Control Facility (RACF). This action was completed by 31 March 1994.

3. Recommendation 3 - Concur.

a. We will develop adequate validity checking for locally written supervisor calls (SVCs) to prevent unauthorized user operations and systems requests that, if allowed, would comprise system security controls. The following actions will be taken in regards to locally-written SVCs:

(1) SVC * will be revised to ensure that RACF checking is done in both paths. Link Pack Area (LPA) and test checking will be removed.

(2) SVC * : We are unaware of the author of this SVC. Parameter library (PARMLIB) comments indicate that this is an IDMS-related SVC. We will take action to capture usage of this SVC and to ascertain its origin. Once this is accomplished, we will request revision or remove the SVC.

Estimated completion date is 31 December 1994.

b. We will remove obsolete SVCs and either correct improperly installed SVCs or replace them with planned upgrades. Any references to * which refer to non-existent SVCs will be removed. In addition, any SVCs identified as obsolete will be removed. We will also address documented deficiencies in SVCs * , * , * , * , * , and * either by applying necessary maintenance or advising that the said deficiencies can only be corrected by program upgrades. If correctable only by program upgrades and no such upgrade is immediately possible, we will then inform higher-level management.

Estimated completion date is 31 December 1994.

4. Recommendation 4 - Concur.

Recommendation 4.a: We will review the security for all primary and secondary integrated data dictionaries and make appropriate changes to verify that application program and data are adequately protected. We activated Security for one secondary dictionary on the Uniform Inventory Control Point (UICP) Production environment (the UICP Resystemization Central Version (URES CV)) that was not activated during the audit. We will review all data dictionary environments on HOST1 that support UICP Development and Test (DATG) and all environments on HOST3 that support UICP Production (POZ) to ensure all dictionaries are protected. In addition, we will also review other IDD Security Features in IDMS 12.0 to ensure these features have been included and implemented on all UICP environments at DMC Mechanicsburg. Estimated completion date is 31 December 1994.

*Supervisor Call numbers deleted.   38

Recommendation 4.b: We will limit batch users with read access for certain IDMS libraries to those users having a valid need. The UICP Production Environment that includes the PX06 Financial Application executes on an Unclassified Processor (POZ). Stricter controls of classified application, executing on the Classified Processor (SECURE), were implemented several years ago. At that time, it was thought controls to even limit read access were not needed in an unclassified environment. Nonetheless, to restrict access to only those users having a valid need, the following steps will be taken:

   a. Access to all IDMS System Libraries that support the UICP environment will be reviewed and "tightened up." These libraries include the following:

	*	*	*
*			

Only DMC Mechanicsburg database management (DBM) personnel and our three Navy Information Service Center (NISC) personnel will be given update authority to these data sets. The DMC DBM and the NISC operate on the UICP Development and Test and Production environments and the UICP Development and Test environment, respectively. If Navy Ships Parts Control Center (SPCC) requires update authority to these data sets, it will be handled on an exception, case-by-case basis for a limited period of time.

   b. Currently, the   *   data set that is needed to access UICP Production Data Bases has a "universal access of read." This data set needs to be referenced in job control language (JCL) for all batch jobs that update or read UICP data in Central Version (CV) mode. However, with the install of IDMS 12.0, any batch job that is submitted by a user is checked by IDMS to insure the batch user is also registered at DMC Mechanicsburg. Universal read access to the   * data set will not be enough to enable a batch user to read or update UICP data. Additionally, IDMS 12.0 Security parameters and features will be analyzed and implemented as appropriate to further control batch access to PX06 financial data.

   c. In conjunction with Navy SPCC, access to certain files containing UICP PX06 financial data will be "RACF protected" to only those access groups with a "need to know." This will further protect batch access to these files in a "local mode retrieval."

ADDITIONAL COMMENTS

   The audit results are consistent in nature and scope with problems discovered in other DoDIG audits performed at five similar facilities which are co-located with the Defense Finance and Accounting Service (DFAS) Centers in Cleveland, Columbus, Denver, Indianapolis, and Kansas City. The problems are systemic and have existed incessantly in every computer center transferred to DISA over the past two years from the Military Departments (MILDEPs), DFAS, and the Defense Logistics Agency (DLA).

*Library and dataset names deleted.

Our capitalization of former MILDEP, DFAS, and DLA computer data centers has provided for the first time, a singularly capable organization with the managerial and professional resources to resolve the long-standing problems that have affected information processing centers (IPCs) across DoD for many years. We first reported IPC deficiencies as an internal management control material weakness for Fiscal Year 1993. The description of the weakness and the milestones for corrections are in the FY93 DoD Annual Statement of Assurance. (Excerpt at enclosure 1.)

This year we will update our progress on correcting this material weakness. Because the problem extends beyond the IPCs, we have expanded the scope of the remedial action to include all DMCs and selected Defense IPCs (DIPCs). We will correct the conditions identified in the audits and proceed further to greatly improve long-term security and technical competence of employees to sustain the improvements and thereby enhance operational efficiency.

Currently, an extensive training program is preparing our work force to better understand operating system controls and security software utilization. When work load migration from the legacy sites has been substantially completed and the expected efficiencies are achieved at each DMC, a comprehensive certification process will be undertaken to qualify each DMC to be accredited by the Director, DISA. In the meantime, each of our DMCs and selected DIPCs have been granted interim authority to operate (IATO) by the Designated Approval Authority (DAA) as of 9 August 1994 (enclosure 2).

Prior to our initiatives, the data processing centers have never been certified and accredited. However, the Assistant Secretary of Defense for Command, Control, Communication and Intelligence recently tasked DISA, the new single manager for information processing systems in DoD, to assemble a task force dedicated to making the data centers proficient. Thus, the DISA Information Security (INFOSEC) Task Force was established in May 1994 and its multi-discipline staff will guide and oversee the effort to upgrade security from inception to completion. The Task Force has already begun reviewing six selected sites.

In the midst of this audit we capitalized DMC Mechanicsburg and began the migration process which involves transferring the work load of eight legacy DIPCs to DISA. A chart depicting the integrated schedule of migration, security and accreditation at DMC Mechanicsburg is at enclosure 3. The DISA INFOSEC Task Force will work in close harmony with the DISA WESTHEM Migration Agent to ensure that the missions of both groups are accomplished in a common sense manner.

The full fledged effort to correct operating system and security software control problems will begin on 13 February 1995 with a DISA WESTHEM Security Readiness Review (SRR) and will continue until 6 April 1995. (An earlier schedule might interfere with the Naval Audit Service audit of general controls which will continue at DMC Mechanicsburg through February 1995.) The SRR will be followed by an on-site visit from a technical team from Computer Associates who will assist in the correction of all

outstanding weaknesses that were either detected by the auditors or by the Task Force. This on-site team may need up to six months to complete their work. The certification process is scheduled to begin in May 1996 and culminate in DISA accreditation in September 1996.

We invited the DoDIG to participate at various in-process reviews conducted by the Task Force and shared the results of the SRRs completed to date and plans for future work. Therefore, we will not reiterate that background information in our comments.

We found the audit team to be knowledgeable in the subject area and positive in their willingness to share valuable information related to the findings and in helping find solutions to the compromises found. The audit team was professional in their approach and methodology. The team's findings and numerous discussions held with DMC Mechanicsburg technical and management personnel has made a significant contribution to improving installation integrity.

DEPARTMENT OF DEFENSE
FISCAL YEAR 1993
STATUS OF CORRECTIVE ACTIONS ON MATERIAL WEAKNESSES

Title and Description of Material Weakness: Operating System
and Security Software Controls. Controls over five of nine
operating system features reviewed at four major Information
Processing Centers (IPCs) needed improvement. Security software
controls were not effectively implemented and management
controls over operating system maintenance and designation of
system programmers positions needed improvement. A
knowledgeable user could access, modify, or destroy sensitive
computer data, programs, and other resources without leaving an
audit trail. Specifically, authorized program facility
libraries and programs were not adequately monitored and
controlled; programmers had installed non-IBM supervisor calls
that compromised system integrity; program names in the program
properties table were not adequately controlled; job entry
subsystem parameters did not control user submission of operator
commands at these major centers, which together process about
$109 billion annually in disbursements.

Functional Category: Information Technology

      Pace of Corrective Action:

Year Identified: 1993

Original Targeted Correction Date: 1994

Targeted Correction Date in Last Year's Report: N/A

Current Target Date: FY 1994

Reason For Change in Date(s): N/A

Component/Appropriation/Account Number: Defense Business
Operations Fund (DBOF)/97X4962

Validation Process: The correction of the material weakness
will be verified through testing as part of a follow up internal
control review of the new controls over operating system and
security software. The Inspector General could assist in this
testing.

Results Indicators: Operations are neither impeded nor
curtailed as a result of the weakness. However, until all
corrective measures are completed, the heightened potential for
catastrophic loss from improper access remains. There are no
potential monetary benefits to be derived from correcting the
control weaknesses found. At this time, performance measures
have not been developed to track the progress, or lack thereof,
of implementing required security controls.

Source(s) Identifying Weakness: Department of Defense Inspector
General Audit Reports Nos. 93-002 and 93-133.

C2-84

Enclosure 1

<u>Major Milestones in Corrective Actions:</u> (C = Corrected)

Completed Milestones:

    Date: Milestone:

    C   IBM recommended installations integrity guidelines
             have been developed for Defense Informations
             Systems Organization (DISO) Information Processing
             Centers (IPCs).

    C   Authorized Program Facility (APF) libraries have
             been reviewed and obsolete and undocumented
             programs have been removed. Also access to APF
             libraries has been limited to the minimum number of
             systems programmers required for maintenance.

    C   Program Property Tables were reviewed and
             obsolete/unneeded entries were nullified; job entry
             subsystem two parameters were reviewed and controls
             put in place to properly control operator commands;
             all obsolete supervisor calls were deleted and an
             improved system has been installed to ensure access
             is restricted to authorized personnel only.

    C   Additional IBM Multiple Virtual Storage with
             Extended Architecture (MVS/XA) operating system and
             IBM Resource Access Control Facility (RACF)
             security software training was conducted.

Planned Milestones (FY 1994):

    Date: Milestone:

    3/94   Publish detailed IBM installation integrity
             guidelines for application in IPCs.

    3/94   Formal written security procedures covering the
             oversight and control of contractor personnel
             working at DISO IPCs will be published; system
             programmer positions in IPCs that require
             "critical-sensitive" designations will be
             identified and action taken to obtain the necessary
             background investigations.

    9/94   Verify correction of material weakness by
             conducting Internal Management Control Reviews of
             IPCs to determine the adequacy of controls over
             operating system and security software supporting
             customer applications.

Planned Milestones (Beyond FY 1994):

             None.

C2-85

43

INTEROFFICE MEMORANDUM

TO: Distribution

FROM: UA

DATE: 0 9 AUG 1994

SUBJECT: Interim Authority to Operate (IATO)

References: (a) DISA Memo, IA, Appointment Memorandum,
                     7 March 1994

                (b) DISAI 630-230-19, Security Requirements for
                     Automated Information Systems (AIS),
                     28 August 1991

1. In accordance with the provisions of the references, I·hereby
grant interim authority to operate (IATO) for the Defense
Megacenters listed in the distribution.

2. Until such time as a complete certification and accreditation
is completed by the Center for Information Systems Security
(CISS), I declare an acceptable level of risk exists to warrant
the continued operation of these Automated Information Systems
Activities.

3. Due to the ongoing migration of systems into the DMCs under
DMR 918 it is not operationally nor economically feasible to
accredit the Megacenters until migration is complete.

4. This IATO remains valid until the CISS accreditation is
completed. However DISO-UAI must be notified if any major change
occurs that could effect security, i.e., a change in processing
mode or classification of data.

                        JOHN M. WATKINS, JR.
                        Brigadier General, USA
                        Director, Defense Information
                            Services Organization

                                              Enclosure 2

DISO, UA, Interim Authority to Operate (IATO),

Distribution:
DMC-CHAMBERSBURG   DMC-OGDEN
DMC-COLUMBUS   DMC-OKLAHOMA CITY
DMC-DAYTON   DMC-ROCK ISLAND
DMC-DENVER   DMC-SACREMENTO
DMC-HUNSTVILLE   DMC-SAN DIEGO
DMC-JACKSONVILLE   DMC-SAN ANTONIO
DMC-MECHANICSBURG   DMC-ST. LOUIS
DMC-MONTGOMERY   DMC-WARNER ROBBINS

Copy to:
UM
UAI

2

DISA "Committed to Excellence"

DISA INFOSEC Task Force
INFOSEC SCHEDULE

DMC MECHANICSBURG

Duration: 981 days 4/15/1994 - 1/16/1998
Security Pkg: RACF/ACF2
Domains: 15

Description	Duration	Start	Finish
DIPC PHILADELPHIA MIGRATION	111	4/15/1994	9/16/1994
DIPC WASHINGTON, D.C. MIGRATION	230	10/17/1994	9/1/1995
DIPC ARLINGTON MIGRATION	239	2/28/1995	1/26/1996
DIPC OCEANA MIGRATION	221	7/28/1995	5/31/1996
DIPC KEY WEST MIGRATION	251	12/1/1995	11/15/1996
DIPC BRUNSWICK MIGRATION	240	5/20/1996	4/18/1997
DIPC MAYPORT MIGRATION	224	10/15/1996	8/22/1997
DIPC PATUXENT RIVER MIGRATION	236	2/21/1997	1/16/1998
SECURITY SURVEY	39	2/13/1995	4/6/1995
SECURITY RPT	18	4/10/1995	5/3/1995
SRR IPR	2	5/18/1995	5/19/1995
ACCREDITATION	90	5/13/1996	9/13/1996

Active Status as of September 9, 1994

9/27/94

12

Enclosure 3

Audit Team Members

Russell A. Rau
David C. Funk
W. Andy Cooley
John A. Dedio
Thomas G. Hare
Frances E. Cain
Dorothy L. Dixon
Phillip L. Holbrook
Susanne B. Allen
Nancy C. Cipolla

47

INTERNET DOCUMENT INFORMATION FORM

A . Report Title   Controls Over Application Software Supporting the Navy's Inventories Held for Sale (NET)

B. DATE Report Downloaded From the Internet: 03/01/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):   OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA   22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 03/01/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.